

Notice of Allowability

Application No.

09/869,966

Examiner

Michael J. Simitoski

Applicant(s)

GUILLOU ET AL.

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the response of 8/17/2006.
2. ☒ The allowed claim(s) is/are 13-24.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date 20061019.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. The response of 8/17/2006 was received and considered.
2. Claims 13-24 are allowed.
3. An Examiner's amendment begins on p. 3 of this action.
4. The Examiner's reasons for allowance being on p. 4 of this action.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Gregory Sebald (612)-336-4728 on 10/23/2006.

The application has been amended as follows:

In claim 14, line 1, please replace "the number" with "a number";

In claim 15, line 1, please replace "the number" with "a number";

In claim 16, line 1, please replace "the $f \cdot m$ " with " $f \cdot m$ ";

In claim 18, line 2, please replace "the number" with "a number";

In claim 19, line 2, please replace "the number" with "a number";

In claim 20, line 2, please replace "the $f \cdot m$ " with " $f \cdot m$ ";

In claim 22, line 2, please replace "the number" with "a number";

In claim 23, line 2, please replace "the number" with "a number";

In claim 24, line 2, please replace "the $f \cdot m$ " with " $f \cdot m$ ".

Allowable Subject Matter

6. Claims 13-24 are allowed.
7. The following is an examiner's statement of reasons for allowance: Similarly to applicant's statement on p. 21 of the response of 9/16/2005, the prior art relied upon fails to teach or suggest determining a modulus equal to the product of at least two prime factors where the second factor is complementary to the first with respect to a chosen base number, calculating public values through $G_i \equiv g_i^2 \bmod n$ and calculating private values by solving either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or $G_i \equiv Q_i^v \bmod n$ where the public exponent v is such that $v = 2^k$ in combination with the other elements of the claim. Menezes discloses choosing prime factors p and q and solving $ed = 1 \bmod (p-1)(q-1)$, but lacks computing multiple private values (§8.2.1). Further, Menezes discloses the prime factors being congruent to 3 mod 4 (§8.7.2). Okamoto teaches generating multiple public and private parameters (p. 36).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

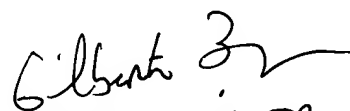
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS



October 20, 2006



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100